Rules

About This Section

Android & Friends

Chrome & Friends

Google & Friends

Open Source

Google Open Source Software Vulnerability Reward Program Rules

Open Source Security Subsidies Rules

OSS-Fuzz Reward Program Rules

Patch Rewards Program Rules

Tsunami Patch Rewards Program Rules

Other

Our Rewards Philosophy

Every week, a group of senior Googlers on our product security team meets to meticulously review and decide reward amounts for all recent bugs reported to us through our Google Vulnerability Reward Program. Based on the researcher's report and the initial triage of the bug by our team, the panel's task is to determine the impact of the given security issue, and to assign a consistent and fair reward amount to every notable find. This article is meant to shed light on how the panel decides rewards for the thousands of vulnerability reports it evaluates, and does not in any form alter the Google VRP rules.

For every reported vulnerability, the security impact is first of all evaluated by looking at the most dangerous attack scenario that the panel can come up with. We usually assign lower severity to problems that hinge on the existence of other, not-yet-discovered bugs to become exploitable; we do the same for findings that require extremely unlikely user interactions or other rarely-met prerequisites. On the flip side, when we can come up with higher-impact attack vectors that the original reporter hadn't considered in the submitted report, we bump up the score accordingly.

In a second step, our evaluation of the security impact then focuses on several additional factors:

- The type of exploit (RCE, XSS etc.), and in particular the kinds of malicious activities the exploit enables (command/SQL injection, sandbox escapes, data exfiltration etc.)
- The sensitivity of the affected application or service. For example, vulnerabilities affecting tier 0 and tier 1 applications as specified in our public list are considered higher impact and are thus eligible for higher rewards than issues affecting applications belonging to lower tiers. That said, if a report demonstrates how a bug in a lower-tier application can lead to an impact equivalent to compromising a higher-tier target (e.g. via some backend

Other aspects of the process worth noting include:

- Over time, we tend to adapt the reward amounts to provide balanced incentives for external researchers – especially as we find that certain classes of targets become more difficult to attack.
- When receiving multiple reports, we typically only reward once per root cause and group similar vulnerabilities together. For example, if there's a service that accidentally disabled CSRF protection, we wouldn't issue a reward for every handler that had CSRF protection disabled, but would instead issue a reward for the most serious CSRF vulnerability in the code.
- We reward exclusively based on security impact – i.e. rewards are not driven by PR, or by legal or reputational risks.
- When a report doesn't technically match the scope, or the impact isn't there, but we appreciate knowing about the issue, or the report led to a change in our products, we'll credit you on our Honorable Mentions board. Examples include bugs in recent acquisitions or bugs in apps that don't deal with user data.
- When in doubt about the exact impact of an issue, we side with researchers and reward the higher amount.
- In some cases, we'll decide to reward duplicate findings, e.g. if the duplicate report significantly contributes to improving the fix or allows us to fix the issue faster.
- A reward is only issued once a quorum of panel members have voted and reached agreement. This can occasionally result in delays as additional complex questions arise.

For more details on how reward amounts are determined, see the rules document for the Google VRP.

While the above description applies specifically to the Google VRP, the basics are the same for all other VRPs at Google: Based on an existing set of rules and an initial triage of the reported issue, a panel comes together to determine the issue's exact severity, and, on that basis, the exact amount that will be rewarded to the researcher who reported the issue.

And now, it's time for you to share your reports for scrutiny by our panel. Good luck bug hunting – we're looking forward to triaging and rewarding your report!